

FIG. 1

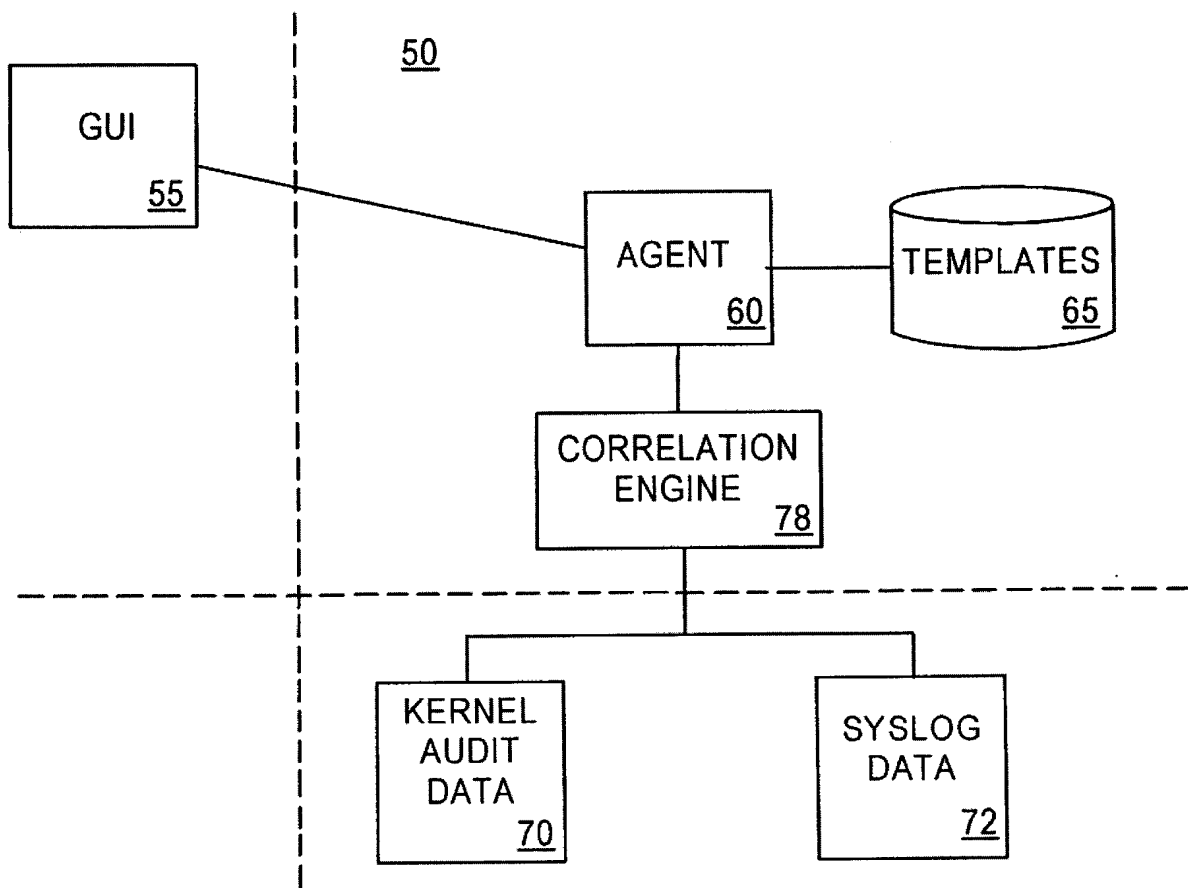


FIG. 2

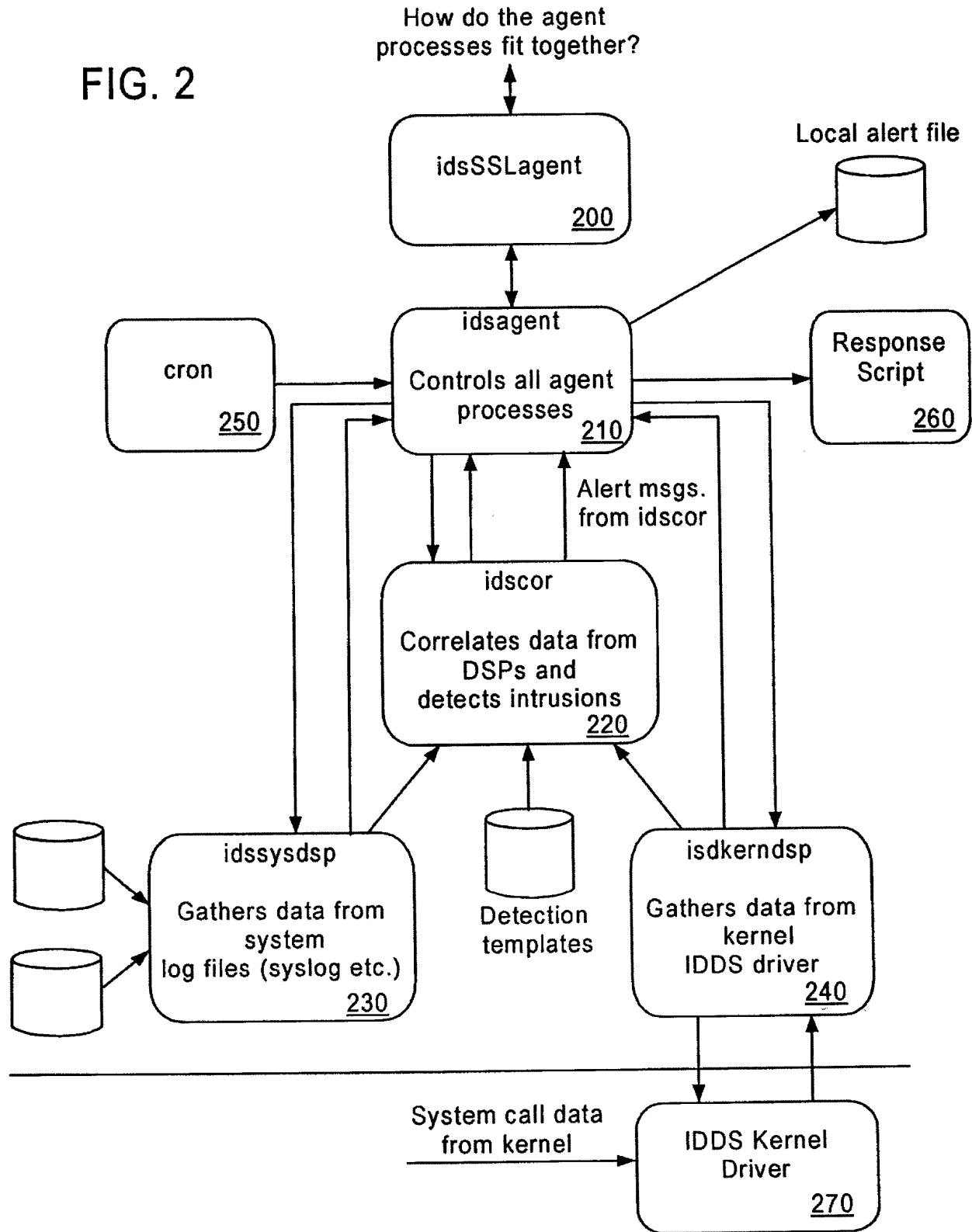
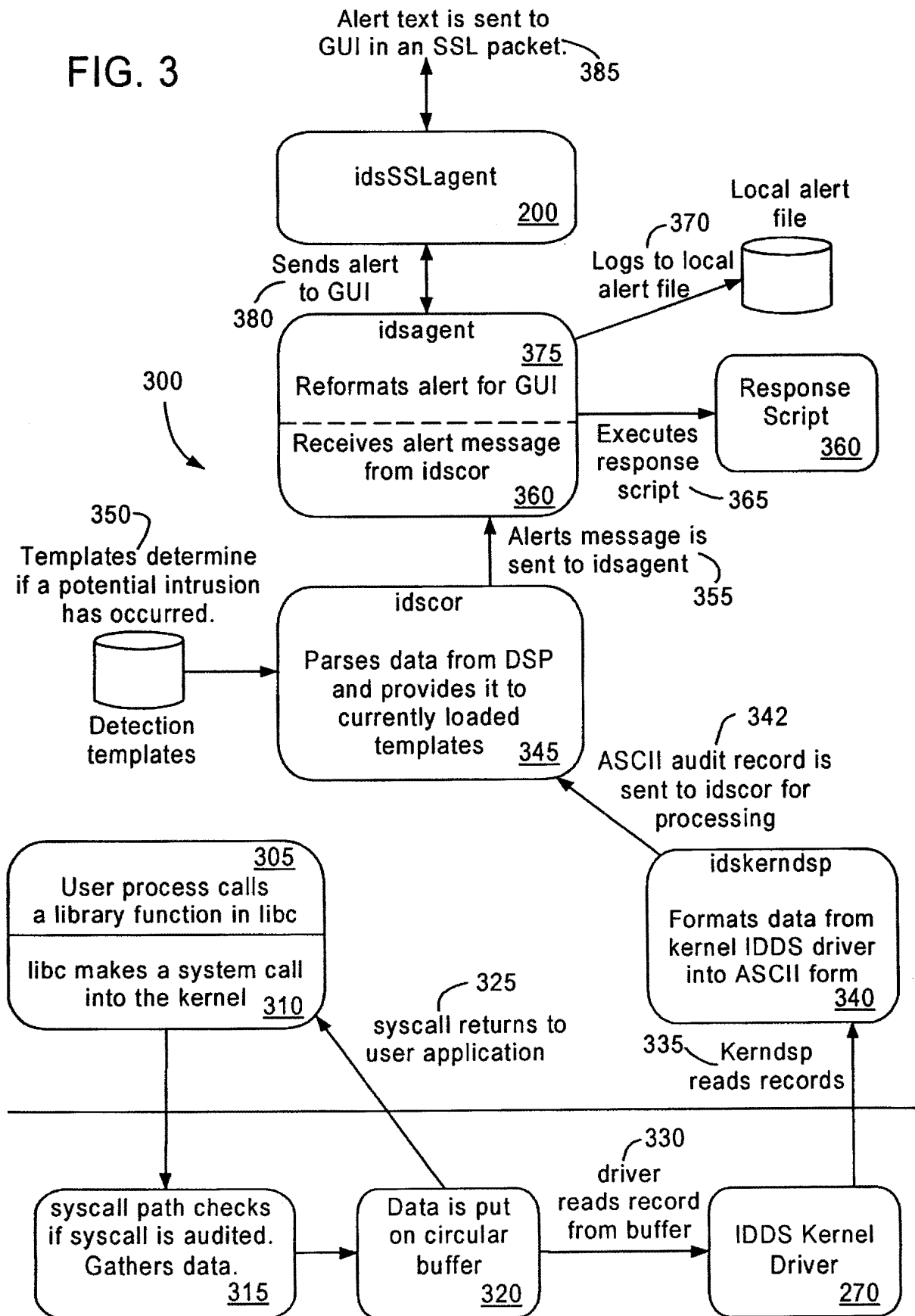
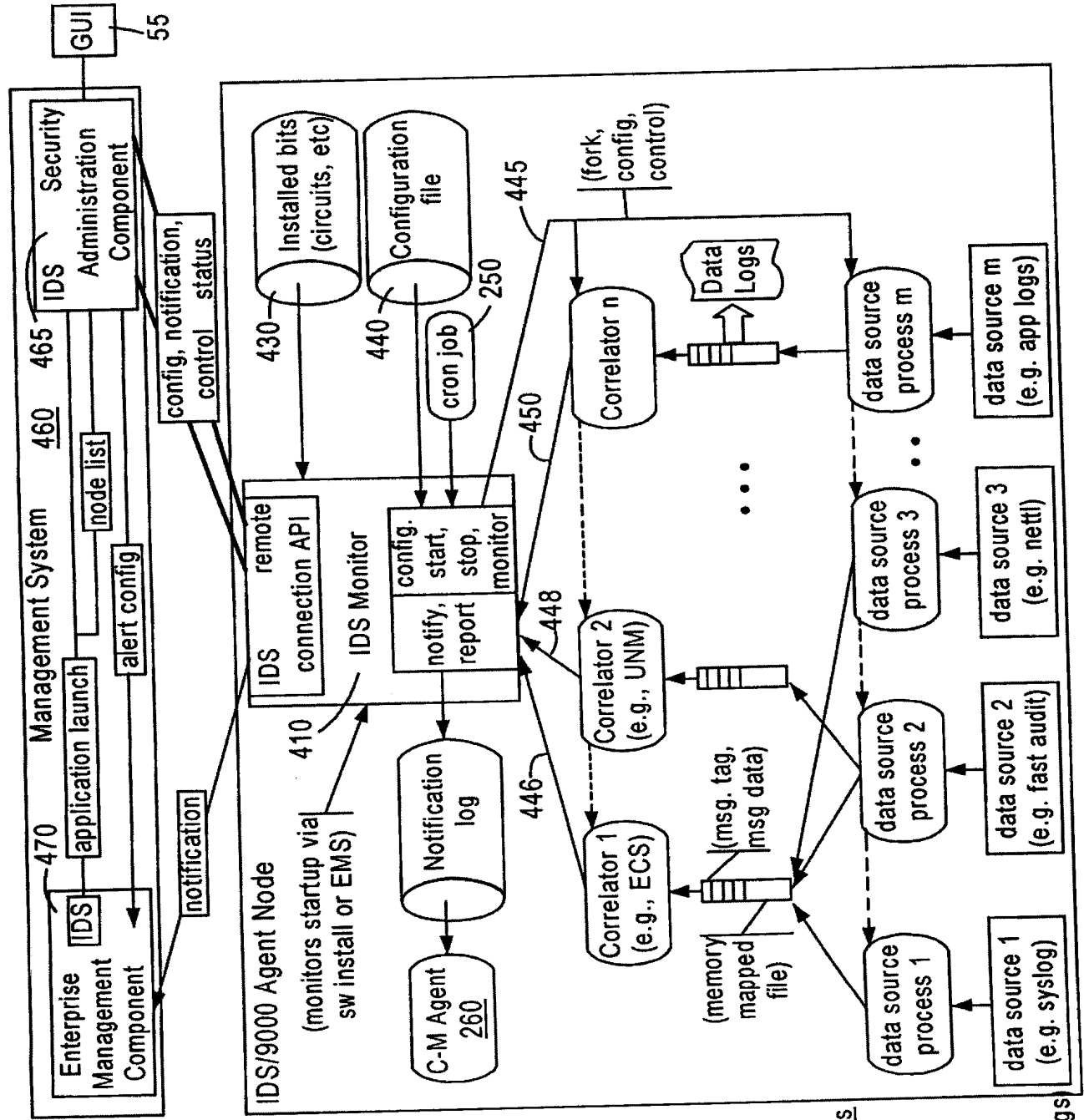


FIG. 3



# FIG. 4



## Infrastructure

- Agent Monitor
- Remote connection

## Operation/Control

- Installation
- Initialization
- Configuration
- Control/Status

## Correlator

- ECS engine core
- Circuit/data control modules
- Messaging control
- Status/Error/Trace output
- Command input and dispatch
- Engine state dump

## Data Source Processes

- Audit
- Syslog
- Network

## Detection Patterns

- Kernel patterns
- Network patterns (future)
- Web server patterns (from logs)

FIG. 5

